U.S. DEPARTMENT OF ENERGY
OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

# Cybersecurity for the Operational Technology Environment (CYOTE) Pilot

Enhancing threat detection in critical operational systems using U.S. Intelligence insights

## Background

Intentional, malicious cyber threats to U.S. energy systems are growing more frequent and more sophisticated. Cyber actors are increasingly targeting critical energy systems with the aim to disrupt physical infrastructure using cyber controls. Identifying risks and detecting attacks on these operational technology (OT) systems requires utilities to know where to look—and what to look for—in complex operating environments.

In contrast with information technology (IT) systems, most utilities lack the capability to collect data from their OT networks, analyze it effectively, and detect attacks in real time.

## Objectives

CYOTE aims to design an industry-led approach for collecting and sharing OT data—one that allows operators to elicit special insights from the U.S. Intelligence Community (IC) and the expertise of DOE National Laboratories.

CYOTE is working with four utilities to pilot a process to identify high-risk OT attack locations, securely share OT network data, and leverage U.S. Intelligence Community capabilities to analyze data to detect sophisticated cyber threats. The pilot will evaluate the feasibility to scale up this process and advance the capability industry-wide.

## Project Description

DOE, working with CYOTE partners, will determine what data to collect and how to securely share sensitive operational data with the IC for enhanced analysis—all the while protecting privacy and meeting cybersecurity regulations. As a result, CYOTE pilots will be industry-driven and flexible—each utility determines the technologies, processes, and approach used to collect, store, process, and share data.

Each pilot will work to:

- Map the OT cyber "kill chain" of potential attack pathways that adversaries could use to compromise the utility OT systems;
- Identify valuable points within the OT system to monitor and share data;
- Install devices at those critical points and identify trusted mechanisms to share key data;
- Analyze operational utility data from the OT environment
- Provide utilities with expert analysis and threat information from the IC that bring classified context to OT threat information; and
- Evaluate the feasibility of a repeatable, industry-wide approach for OT threat data analysis.

## Benefits

- Establishes a repeatable, industry-wide approach for OT threat data analysis
- Provides utilities with expert analysis and threat information from the U.S. intelligence community that bring classified context to OT threat information
- Identifies the cyber kill-chain in OT systems that are vulnerable to compromise

## Partners

- Idaho National Laboratory (lead)
- Argonne National Laboratory
- Oak Ridge National Laboratory
- Pacific Northwest National Laboratory

## Period of Performance

August 2016 – September 2019

### Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber-attacks.

### Contact Information:

Akhlesh Kaushiva, P.E.
Program Manager
DOE CESER
202-287-6062
Akhlesh.Kaushiva@Hq.Doe.Gov

Robert Smith
Principal Investigator
Idaho National Laboratory
208-526-3881
Robert.Smith@inl.gov

### For More Information:

https://www.energy.gov/ceser

## Pilot Approach

The CYOTE pilot aims to

- Produce a **template for collecting and sharing OT data** for generation, transmission, and distribution networks
- **Identify and install advanced devices and share and analyze OT data streams** using Intelligence Community tools and insights.
- Determine **whether CYOTE analysis can provide actionable information to help utilities defend their networks** against sophisticated attacks.
- Identify and **recommend a methodology to expand CYOTE analysis** into a rapid, industry-wide capability.

## Anticipated Results

- Optimally deployed devices at effective nodes for data collection and system monitoring
- Advanced devices that can distinguish adversary activity from noise
- Trusted mechanisms for utilities to share key sensitive data items and patterns
- Evaluation of where U.S. Intelligence can deliver new insights

August 2018